考虑量化不匹配问题的信息物理系统的安全控制 *

贾欣婷[a]，郑柏超[a, b]，裴　斌[a]
(南京信息工程大学 a. 自动化学院; b. 江苏省大气环境与装备技术协同创新中心, 南京 210044)

摘　要: 针对一类包含执行器攻击、外部干扰和编码器/解码器不匹配的信息物理系统(cyber-physical systems, CPS)，设计一种新型鲁棒控制器确保其安全稳定运行。控制器线性部分的增益由优化 H2 性能的线性矩阵不等式给出；控制器的非线性结构包含两部分,一部分用于消除外部干扰、量化误差，另一部分利用对未知执行器攻击参数的自适应估计来实现对攻击的补偿。最后，仿真算例结果表明控制器能保证闭环系统的一致最终有界性，说明了所提方法的有效性。

关键词: 信息物理系统；执行器攻击；编码器/解码器失配；一致最终有界
中图分类号: TP273.3　　doi: 10.19734/j.issn.1001-3695.2018.11.0890

Security control of cyber-physical systems considering quantization mismatch

Jia Xinting[a], Zheng Bochao[a, b], Pei Bin[a]
(*a. School of Automation*, *b. Jiangsu Collaborative Innovation Center on Atmospheric Environment & Equipment Technology*, *Nanjing University of Information Science & Technology*, *Nanjing* 210044, *China*)

Abstract: This paper proposed a novel robust controller to ensure the security and stability for a class of cyber-physical systems subject to the effects including actuator attacks, external disturbances, and encoder/decoder mismatches. An optimized H2 performance in the form of linear matrix inequality solves the linear gain of the constructed controller. The nonlinear structure of the control includes two parts: one aims to eliminate the influence of external disturbance and quantization error, and the other part compensates the actuator attack by means of adaptive estimations of unknown actuator attack parameters. Finally, the simulation results show that the controller guarantees uniform ultimate boundedness of the closed-loop dynamical system, which shows the effectiveness of the proposed method.

Key words: cyber-physical system; actuator attacks; encoder/decoder mismatch; uniform ultimate boundedness

0　引言

随着信息技术的飞速发展及其数据处理能力的不断提升，使通信和控制系统越来越紧密地联合在一起，信息物理系统(cyber-physical systems,CPS)作为一种新型智能系统应运而生[1]。CPS 集成了物理过程，计算资源和通信功能，本质上是具有控制属性的网络，将物理设备连上互联网，但 CPS 更强调循环反馈。尽管 CPS 具有良好的广泛的应用前景[2]，但仍然有许多不足之处需要解决，尤其是安全方面的问题[3~6]。

由于 CPS 使用开放的计算和通信平台架构，很容易受到敌对攻击，攻击者可以访问传感和驱动计算平台，操纵系统测量数据和控制输入命令，严重影响系统的性能和完整性，因此 CPS 中的安全性比一般计算系统更重要[7]。对于 CPS 的可靠控制问题，针对考虑传感器攻击的 CPS，Yucelen 等人[8]提出了自适应控制器以确保系统的稳定性。针对考虑执行器攻击和噪声的 CPS，Xie 等人[9]提出了新颖的切换观测器以确保系统的稳定性。针对同时考虑传感器和执行器攻击的 CPS，Jin 等人[10]提出了自适应控制器以确保系统的稳定性。

由于数字通信信道在现代工业控制系统中的广泛应用，而通信网络又往往受到通信带宽、有限数据率等困扰，所以通常需要对所测得的信息进行量化处理[11]。信号量化的过程可以看做是编码和解码的过程，编码器和解码器的量化参数必须是相等，Yun 等人[12]研究了具有输入量化和外部扰动的不确定线性系统的 H_2 状态反馈控制器的设计。由于硬件执行的不理想，在实践中可能会导致量化过程中编码和解码的量化参数不一致的问题。针对此缺陷，Zheng 等人[13]研究了具有量化参数不匹配的线性系统的 H_2 控制器的设计。

然而，在 CPS 的分析与控制的研究中，极少有考虑含信号量化，特别是量化编解码不一致的成果发表。为此，本文研究执行器攻击模式下的含模型不确定[14]的 CPS，并同时考虑量化不匹配问题，通过设计控制器以确保系统的稳定性。控制器的线性部分使模型不确定和量化不匹配的系统实现鲁棒 H_2 性能，非线性部分用于消除外部干扰、量化误差以及抑制或抵消状态相关的执行器攻击对系统的影响，从而保证闭环系统的一致最终有界性。

1　预备知识及问题描述

1.1　预备知识

首先介绍本文会用到的投影 $\mathrm{Proj}: R^n \times R^n \to R^n$ 。给出一个连续可微的凸函数为 $\phi(\theta) =: \frac{(\varepsilon_\theta+1)\theta^T\theta-\theta_{\max}^2}{\varepsilon_\theta\theta_{\max}^2}$ ，其中 $\theta_{\max} \in R$ 是 $\theta \in R^n$ 的投影范数界，$\varepsilon_\theta > 0$ 是投影容差界限，对于 $y \in R^n$，向

收稿日期: 2018-11-26；**修回日期:** 2019-01-14　**基金项目:** 国家自然科学基金资助项目（61573189，61403207）；中国博士后科学基金资助项目（2015M580380）

作者简介: 贾欣婷（1995-），女，江苏扬州人，硕士研究生，主要研究方向为信息物理系统的安全控制问题（jiaxinting_7@163.com）；郑柏超（1981-），男，山东烟台人，副教授，硕导，博士，主要研究方向为滑模控制，网络量化控制；裴斌（1995-），男，江苏扬州人，硕士研究生，主要研究方向为微电网控制.

量的投影定义为

$$\mathrm{Proj}(\theta,y)=:\begin{cases} y & \text{if } \phi(\theta)<0 \\ y & \text{if } \phi(\theta)\ge 0, \phi'(\theta)y\le 0 \\ y-\dfrac{\phi'^T(\theta)\phi'(\theta)y}{\phi'(\theta)\phi'^T(\theta)}\phi(\theta) & \text{if } \phi(\theta)\ge 0, \phi'(\theta)y>0 \end{cases} \quad (1)$$

在向量的投影基础上，定义矩阵的投影 $\mathrm{Proj}_m: R^{n\times m}\times R^{n\times m}\to R^{n\times m}$

$$\mathrm{Proj}_m(\Theta,Y)=(\mathrm{Proj}(\mathrm{col}_1(\Theta),\mathrm{col}_1(Y)),\cdots,\mathrm{Proj}(\mathrm{col}_m(\Theta),\mathrm{col}_m(Y))) \quad (2)$$

其中: $\Theta\in R^{n\times m}$， $Y\in R^{n\times m}$， $\mathrm{col}_i(A)$ 表示矩阵 A 的第 i 列。

文中 R 表示实数集合， R^n 表示 n 维实数列向量， $R^{n\times m}$ 表示 $n\times m$ 维的实矩阵，A^T 表示矩阵 A 的转置，A^{-1} 表示矩阵 A 的逆矩阵， $X>0(X\ge 0)$ 表示 X 是正定（半正定）矩阵，$\|\cdot\|_p$ 表示向量的 p -范数，即 $\|x\|_p=(\|x_1\|^p+\|x_2\|^p+\cdots+\|x_n\|^p)^{1/p}$， $p\ge 1$，当 $p=\infty$ 时， $\|x\|_\infty=\max_{1\le i\le n}\|x_i\|$， 特别的， $\|\cdot\|$ 表示 2-范数， $\|\cdot\|_F$ 表示 Frobenius 矩阵范数， $\bar{x}(\underline{x})$ 表示 x 的上界（下界），对称矩阵的对称位置用“*”表示。

1.2 问题描述

针对遭受执行器攻击的不确定信息物理系统，建立如式（3）所示的动态方程模型。

$$\dot{x}(t)=(A+\Delta A(t))x(t)+B\tilde{u}(t)+B\omega(t) \quad (3)$$

其中：$x(t)\in R^n$ 表示系统的状态，$\omega(t)\in R^m$ 是外部干扰， A 和 B 为已知的具有适当维数的常值矩阵，$\Delta A(t)$ 是适当维数的不确定参数矩阵，$\tilde{u}(t)\in R^m$ 为遭受执行器攻击的控制输入，其数学表达式为

$$\tilde{u}(t)=u(t)+\delta_a(t,x(t)) \quad (4)$$

其中: $\delta_a(t,x(t)):R\times R^n\to R^m$ 为攻击模式，是发生在控制器与执行器之间通信链路上的攻击。同文献[10]一样，本文假设执行器攻击参数化为 $\delta_a(t,x(t))=W^T(t)\varphi(x(t))$， 其中， $W(t)\in R^{p\times m}$ 是未知的时变加权矩阵且 $\|W(t)\|_F\le\bar{W}$, $\|\dot{W}(t)\|_F\le\bar{\dot{W}}$ ， $\varphi(x(t))\in R^p$ 是结构已知的关于 $x(t)$ 的非线性函数。从表达式（2）可见，如果 $\delta_a(\cdot,\cdot)$ 非零，则控制输入信号 $u(t)$ 会被错误（或恶意）的信号 $\tilde{u}(t)$ 取代，即，系统遭受执行器攻击。

另一方面，控制系统的执行过程越来越多的采用远程通信或数字方式来实现，而数字通信网络往往受到通信带宽、有限数据率等困扰，所以通常需要对所测得的信息进行量化处理。量化器 $Q(\cdot)$ 由向最接近的整数舍入函数 $q(\cdot)$ 定义，本文采用如下的量化器形式：

$$Q(u(t))=\mu_d(t)q\left(\frac{u(t)}{\mu_c(t)}\right) \quad (5)$$

其中，$\mu_d(t)$ 和 $\mu_c(t)$ 分别为编码侧和解码侧的量化灵敏度参数，令 $r(t)=\mu_d(t)/\mu_c(t)$，理想情况下 $\mu_d(t)$ 和 $\mu_c(t)$ 是相等的，即 $r=1$。然而在实际控制工程中，由于硬件执行不理想，该要求显然是非常严格且难以实施的，所以本文考虑量化不匹配更一般的情况，$r(t)\in(\underline{r},\bar{r})$，其中，$\underline{r}$ 和 $\bar{r}$ 都是正参数并且 $\bar{r}\ge 1\ge\underline{r}>0$，所以 $r=1$ 也是该情况下的一种特殊情况。

综合上述式（3）~（5），系统（3）变为式（6）的形式

$$\dot{x}(t)=(A+\Delta A(t))x(t)+BQ(\tilde{u}(t))+B\omega(t) \quad (6)$$

其中 $Q(\tilde{u}(t))$ 是受到执行器攻击的量化输入

$$Q(\tilde{u}(t))=\mu_d(t)\left[q\left(\frac{u(t)}{\mu_c(t)}\right)+\delta_a(t,x(t))\right] \quad (7)$$

在信息物理系统（6）的运行过程中，控制输入 $u(t)$ 经编码器一侧获得量化测量信息 $q(u(t)/\mu_c(t))$，在传输编码过的控制信号到解码器处的网络通信链路中，受到网络攻击者恶意注入的执行器攻击 $\delta_a(t,x(t))$，在传输到执行器之前的控制信号需要先进行解码，经解码器获得遭受执行器攻击的量化输入 $Q(\tilde{u}(t))$，量化反馈的信息物理系统如图 1 所示。

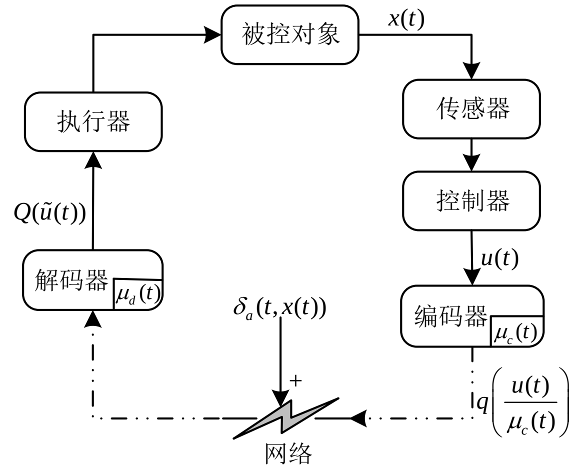


图 1 信息物理系统结构图

Fig. 1 Structure diagram of cyber-physical system

首先给出以下 3 个假设：

假设 1 系统（ A , B ）是可控的。

假设 2[13] 时变的不确定矩阵 $\Delta A(t)$ 满足

$$\Delta A(t)=F_1\Delta(t)E_1,\ \Delta(t)\Delta(t)^T\le I \quad (8)$$

其中： F_1 和 E_1 是已知的具有适当维数的常值矩阵， $\Delta(t)$ 是未知的时变矩阵。

假设 3[13] 存在已知的参数 ε_ω 使得外部干扰 $\omega(t)$ 满足

$$\|\omega(t)\|_\infty\le\varepsilon_\omega \quad (9)$$

在给出本文的控制器设计之前，首先引入如下的 H_2 性能指标的概念[12]：

$$J(t)=\int_t^\infty\{x^T(s)Qx(s)+x^T(s)K^TRKx(s)\}ds \quad (10)$$

其中： Q 和 R 是给定的对称正定加权矩阵， K 是控制器中给出的线性反馈增益矩阵。

本文用到如下三个引理。

引理 1[12] 对于任意两个 n 维实向量 α 与 β ， 当 $p\ge 1$ ， $q\ge 1$ 且 $p^{-1}+q^{-1}=1$ 时， 下列不等式成立

$$\|\alpha^T\beta\|\le\|\alpha\|_p\|\beta\|_q$$

引理 2[15] 对于任意给定适当维数的实矩阵 Π 、X 和 Y ， 其中 Π 是对称的， 当矩阵 $F(t)$ 满足 $F^T(t)F(t)\le I$ 时， 则

$$\Pi+XF(t)Y+Y^TF(t)^TX^T<0$$

当且仅当存在一个常数 $\varepsilon>0$ 使得下列不等式成立

$$\Pi+\varepsilon XX^T+\varepsilon^{-1}Y^TY<0$$

引理 3[10] 根据矩阵投影 Proj_m 的定义， 对于给定的 $\Theta^*\in R^{n\times m}$， 下列不等式成立：

$$\mathrm{tr}((\Theta-\Theta^*)^T(\mathrm{Proj}_m(\Theta,N)-N))\le 0$$

2 量化不匹配 CPS 的安全控制

针对上述信息物理系统式（6）设计一种新型鲁棒控制器保证闭环系统的一致最终有界性。其线性部分的增益由优化 H_2 性能的线性矩阵不等式给出；其非线性部分用于消除外部干扰、量化误差以及抑制或抵消状态相关的执行器攻击对系统的影响。构造如下结构的控制器

$$u(t)=Kx(t)+u_n(t)+v(t) \quad (11)$$

其中：

$$u_n(t) = -(\frac{\mu_c}{2} + \frac{\varepsilon_\omega}{\underline{r}})\mathrm{sign}(x^T PB) \tag{12}$$

$$v(t) = -\mu_c \hat{W}(t)^T \varphi(x(t)) \tag{13}$$

$\hat{W}(t)$ 满足自适应律：

$$\dot{\hat{W}}(t) = \eta \bar{r} \mu_c \mathrm{Proj}_m(\hat{W}(t), \varphi(x(t))x^T PB) \tag{14}$$

参数 η 为正的调节增益， Proj_m 为矩阵的投影。

$Kx(t)$ 为线性部分,用于使不确定性系统实现如式(10)的 H_2 性能。

$u_n(t)$ 与 $v(t)$ 为非线性部分,分别用来处理量化误差和外部干扰、抑制或抵消状态相关的执行器攻击的影响。

为了证明方便，定义 $\tilde{W} = W - \hat{W}$ ， $e_{\mu_c} = \mu_c q\left(\frac{u}{\mu_c}\right) - u$ ，容易得到：

$$\begin{aligned}\dot{x} &= (A + \Delta A(t))x(t) + B[\frac{\mu_d}{\mu_c}\mu_c(q(\frac{u}{\mu_c}) + \delta_a(t, x(t)))] + B\omega(t) \\ &= (A + F_1\Delta_1 E_1)x(t) + rB[u + e_{\mu_c} + \mu_c W^T(t)\varphi(x(t))] + B\omega(t) \\ &= (A + F_1\Delta_1 E_1)x(t) + rB[Kx(t) + u_n + e_{\mu_c} + \mu_c \tilde{W}^T(t)\varphi(x(t))] \\ &\quad + B\omega(t)\end{aligned}$$

和
$$\dot{\tilde{W}}(t) = \dot{W}(t) - \eta \bar{r} \mu_c \mathrm{Proj}_m(\hat{W}(t), \varphi(x(t))x^T PB)$$

定理 1　对于满足假设 1~3 的信息物理系统式（6）并且 $\delta_a(t, x(t)) = 0$ ，当 $r \in (\underline{r}, \bar{r})$ 时，存在对称正定矩阵 $\bar{P}$ 和 M ，常规矩阵 $\bar{K}$ ，正标量 η_1 ，使以下的优化问题有解。

$$\min \quad \mathrm{Trace}(M)$$

$$\begin{bmatrix} \Gamma & \bar{P}E_1^T & \bar{P} & \bar{K}^T \\ * & -\eta_1 I & 0 & 0 \\ * & * & -Q^{-1} & 0 \\ * & * & * & -R^{-1} \end{bmatrix} < 0 \tag{15}$$

$$\begin{bmatrix} M & I \\ I & \bar{P} \end{bmatrix} > 0 \tag{16}$$

其中：$\Gamma = A\bar{P} + \bar{P}A^T + \eta_1 FF^T + rB\bar{K} + r\bar{K}^T B^T$ 。当 $K = \bar{K}\bar{P}^{-1}$ 时，则由式（11）给出的满足式（12）的控制器使闭环系统 $x(t)$ 轨迹渐近收敛于原点并满足 H_2 性能，可以通过最小化矩阵 M 的迹来达到最小的 H_2 性能上界。

证明　考虑李雅普诺夫函数 $V = x(t)^T Px(t)$ ， $V(t)$ 沿系统轨迹的时间导数为

$$\begin{aligned}\dot{V} &= \dot{x}^T Px + x^T P\dot{x} \\ &= x^T[(A + F_1\Delta_1 E_1)^T P + P(A + F_1\Delta_1 E_1) + rK^T B^T P + rPBK]x \\ &\quad + 2rx^T PB(u_n + e_{\mu_c}) + 2x^T PB\omega(t)\end{aligned}$$

根据引理 1，假设 2、3，因为不等式

$$\|e_{\mu_c}\|_\infty = \left\|\mu_c q\left(\frac{u}{\mu_c}\right) - u\right\|_\infty = \left\|\mu_c(q(\frac{u}{\mu_c}) - \frac{u}{\mu_c})\right\|_\infty \le \mu_c/2$$

可得

$$\begin{aligned}&2rx^T PB(u_n + e_{\mu_c}) + 2x^T PB\omega \le \\ &\quad 2rx^T PBu_n + 2r\|x^T PB\|_1 \|e_{\mu_c}\|_\infty + 2\|x^T PB\|_1 \|\omega\|_\infty \le \\ &\quad 2rx^T PBu_n + 2r\|x^T PB\|_1 \frac{\mu_c}{2} + 2\|x^T PB\|_1 \varepsilon_\omega\end{aligned} \tag{17}$$

将式（12）代入式（17）可得

$$2rx^T PBu_n + 2r\|x^T PB\|_1 \frac{\mu_c}{2} + 2\|x^T PB\|_1 \varepsilon_\omega \le 0$$

根据引理 2 可得

$$\begin{aligned}&(A + F_1\Delta_1 E_1)^T P + P(A + F_1\Delta_1 E_1) + rK^T B^T P + rPBK \le \\ &\quad A^T P + PA + \eta_1^{-1}E_1^T E_1 + \eta_1 PF_1 F_1^T P + rPBK + rK^T B^T P\end{aligned}$$

所以

$$\dot{V} \le x^T(A^T P + PA + \eta_1^{-1}E_1^T E_1 + \eta_1 PF_1 F_1^T P + rPBK + rK^T B^T P)x$$

如果不等式

$$\begin{aligned}&A^T P + PA + \eta_1^{-1}E_1^T E_1 + \eta_1 PF_1^T F_1 P \\ &\quad + rK^T B^T P + rPBK + Q + K^T RK < 0\end{aligned} \tag{18}$$

成立，可以得到

$$\dot{V}(t) \le -x^T(t)(Q + K^T RK)x(t) \le \dot{J}(t)$$

由于 $J(\infty) = V(\infty) = 0$ 以及 $\dot{V}(t) \le \dot{J}(t)$ ，可以得到 $J(t) \le V(x(t)) \le V(x(0))$ ，从上述结论可以看出 H_2 性能的上界依赖于系统的初始状态 $x(0)$ ，而在实际应用中，很难精确确定系统的初始状态，为了克服这一困难，可以假定初始状态 $x(0)$ 是一个满足 $\mathrm{E}\{x(0)x^T(0)\} = I$ 的零均值随机变量。通过考虑性能指标的期望值，得到

$$\bar{J} = \mathrm{E}\{J\} \le \mathrm{E}\{x(0)Px^T(0)\} = \mathrm{Trace}(P)$$

根据 Schur 补引理[12]，定理 1 中的约束条件式（16）等价于 $M > P > 0$，因此，M 的迹最小化将保证 P 的迹的最小化，即系统 H_2 性能上界的最小化。在式（18）两边同乘以 P^{-1} ，令 $\bar{P} = P^{-1}$ 以及 $K = \bar{K}\bar{P}^{-1}$，根据 Schur 补引理，可以得到如式（15）的不等式。因此，通过最小化正定矩阵 $\bar{P}$ 、M 、常规矩阵 K 、正标量 η_1，可以实现最小 H_2 性能上界，由此定理 1 证明完毕。

定理 2　对于满足假设 1~3 的信息物理系统式（6），对于所有 $(x(0), \tilde{W}(0)) \in R^n \times R^{p\times m}$ ，由式（11）给出的满足式（12）~（14）的控制器使闭环系统是一致有界的，且 $x(t)$ 和 $\tilde{W}(t)$ 最终有界。

$$\|x(t)\| \le [\frac{1}{\lambda_{\min}(P)}(\lambda_{\max}(P)d_1^{-1}d_2 + \eta^{-1}(\bar{W} + \hat{W}_{\max})^2)]^{\frac{1}{2}} \tag{19}$$

$$\|\tilde{W}(t)\|_F \le [\eta\lambda_{\max}(P)d_1^{-1}d_2 + (\bar{W} + \hat{W}_{\max})^2]^{\frac{1}{2}} \tag{20}$$

其中： $d_1 = \lambda_{\min}(Q + K^T RK)$ ， $d_2 = \frac{2(r - \bar{r})}{\eta\bar{r}}(\bar{W} + \hat{W}_{\max})\dot{\hat{W}}_{\max} + 2\eta^{-1}(\bar{W} + \hat{W}_{\max})\dot{\bar{W}}$ ， $\hat{W}_{\max} \in R$ ， $\dot{\hat{W}}_{\max} \in R$ 是投影的范数界。

证明　考虑李雅普诺夫函数 $V = x(t)^T Px(t) + \eta^{-1}tr(\tilde{W}^T(t)\tilde{W}(t))$ ，前面的证明类似定理 1， $V(t)$ 沿系统轨迹的时间导数是

$$\begin{aligned}\dot{V} &= \dot{x}^T Px + x^T P\dot{x} + 2\eta^{-1}tr(\tilde{W}^T\dot{\tilde{W}}) \le \\ &\quad -x^T(Q + K^T RK)x + 2rx^T PB(\mu_c \tilde{W}^T\varphi(x(t))) \\ &\quad -2\bar{r}\mu_c tr[\tilde{W}^T \mathrm{Proj}_m(\hat{W}, \varphi(x(t))x^T PB)] + 2\eta^{-1}tr(\tilde{W}^T\dot{W})\end{aligned}$$

根据引理 3 可得

$$\begin{aligned}&2rx^T PB(\mu_c\tilde{W}^T\varphi(x(t))) - 2\bar{r}\mu_c tr[\tilde{W}^T \mathrm{Proj}_m(\hat{W}, \varphi(x(t))x^T PB)] = \\ &2r\mu_c tr[\tilde{W}^T\varphi(x(t))x^T PB] \\ &\quad -2(r - r + \bar{r})\mu_c tr[\tilde{W}^T \mathrm{Proj}_m(\hat{W}, \varphi(x(t))x^T PB)] = \\ &2r\mu_c tr[(\hat{W} - W)^T(\mathrm{Proj}_m(\hat{W}, \varphi(x(t))x^T PB) - \varphi(x(t))x^T PB)] \\ &\quad +2(r - \bar{r})\mu_c tr[\tilde{W}^T \mathrm{Proj}_m(\hat{W}, \varphi(x(t))x^T PB)] \le \\ &2(r - \bar{r})\mu_c tr[\tilde{W}^T \mathrm{Proj}_m(\hat{W}, \varphi(x(t))x^T PB)]\end{aligned}$$

所以

$$\begin{aligned}\dot{V} &\le -x^T(Q + K^T RK)x + \frac{2(r - \bar{r})}{\eta\bar{r}}tr(\tilde{W}^T\dot{\hat{W}}) + 2\eta^{-1}tr(\tilde{W}^T\dot{W})\|x\|^2 \le \\ &\quad -d_1\|x\|^2 + d_2\end{aligned}$$

因此，在 Ω 集合之外， $\dot{V} < 0$ 。

$$\Omega = \{(x(t), \tilde{W}(t)) \in R^n \times R^{p\times m} : \|x(t)\| \le \vartheta_1, \|\tilde{W}(t)\|_F \le \vartheta_2\}$$

其中 $\vartheta_1 = \sqrt{d_2/d_1}$ ， $\vartheta_2 = \bar{W} + \hat{W}_{\max}$ ，这就证明了定理 2 闭环系统的

一致有界性。

因为

$$\lambda_{\min}(P)\|x(t)\|^2+\eta^{-1}\|\tilde{W}\|_F^2\le\upsilon_{\max} \tag{21}$$

其中：$\upsilon_{\max}=\lambda_{\max}(P)\vartheta_1^2+\eta^{-1}\vartheta_2^2$，由式（21）可得 $\|x(t)\|^2\le\frac{\upsilon_{\max}}{\lambda_{\min}(P)}$，$\|\tilde{W}\|_F^2\le\eta\upsilon_{\max}$，所以 $x(t)$ 和 $\tilde{W}(t)$ 是最终有界的，由此定理 2 证明完毕。

3　实验结果与分析

下面给出一个仿真实例来验证本文所提方法的有效性。考虑如式(6)形式的飞行器动态系统的线性化模型[10]，其中，系统状态 $x(t)=[\beta(t),p(t),\gamma(t)]^T$ 包含侧滑角（deg）、滚转率（deg/s）以及偏航率（deg/s），控制输入 $u(t)=[\delta_{ail}(t),\delta_{rud}(t)]^T$ 包含副翼偏转（deg）以及方向舵偏转（deg），系统的矩阵参数如下：

$$A=\begin{bmatrix}-0.025&0.104&-0.994\\574.7&0&0\\16.20&0&0\end{bmatrix},\ B=\begin{bmatrix}0.122&-0.276\\-53.61&33.25\\195.5&-529.4\end{bmatrix}$$

$$F_1=[1\ \ 0\ \ 5]^T,\ E_1=[1\ \ 1\ \ 1]$$

仿真中考虑三种情况。

a)为了说明量化不匹配问题对系统稳定性的影响，先进行量化灵敏度参数匹配时的信息物理系统的仿真，对称正定矩阵 P 和控制器增益 K 由文献[12]定理 3 中的 *LMIs* 求出，控制器中的非线性补偿器 $u_n(t)$ 采用文献[12]的形式。

b)同上述的对称正定矩阵 P、控制器增益 K 选取以及补偿器 $u_n(t)$ 的形式相同，将量化灵敏度参数修改为不匹配时，对信息物理系统进行仿真。

c)针对上述修改为不匹配的量化灵敏度参数，由本文定理 1 中的 *LMIs* 求解给出对称正定矩阵 P 和控制器增益 K，控制器中的补偿器 $u_n(t)$ 如（12）的形式进行仿真。

情况 1　根据文献[12]中的定理 3，选取参数矩阵 $Q=0.01I_3$，$R=0.1I_3$，求得

$$P=\begin{bmatrix}2.8242&0.0971&-0.0102\\0.0971&0.0043&0.0001\\-0.0102&0.0001&0.0006\end{bmatrix},\ K=\begin{bmatrix}35.4708&1.4384&-0.0406\\6.4268&0.4774&0.2267\end{bmatrix}$$

选取量化灵敏度参数 $\mu_d=\mu_c=0.06$，假设执行器攻击为 $\delta_a(t,x(t))=[0.5\sin t\quad\cos(2t)]^T\,0.2\sin(\beta(t))\cos(p(t))$。运用 Matlab / Simulink 对系统（6）进行仿真，得到系统的响应曲线如图 2 和图 3 所示。可以看出，当量化器灵敏度参数匹配时，文献[12]的控制器使信息物理系统的状态和控制输入收敛于原点，系统趋近于稳定。

情况 2　选取量化灵敏度参数分别为 $\mu_d=0.06$ 和 $\mu_c=0.1$，运用 Matlab/Simulink 进行仿真，得到系统的响应曲线如图 4 和 5 所示，仿真结果看出，由于编码器和解码器量化灵敏度参数发生不匹配现象，闭环系统状态是发散的，系统呈现不稳定现象，文献[12]的方法失效。

情况 3　根据本文定理 1，可求得

$$P=\begin{bmatrix}0.9312&0.0369&0.0030\\0.0369&0.0024&0.0008\\0.0030&0.0008&0.0007\end{bmatrix},\ K=\begin{bmatrix}19.0594&-0.3813&-1.3382\\9.5125&5.1038&4.9255\end{bmatrix}$$

运用本文定理 2 中的控制器设计方法，并经 MATLAB /Simulink 对闭环系统进行仿真，系统的响应曲线如图 6 和 7 所示，仿真结果表明设计的控制器在信息物理系统发生量化灵敏度参数不匹配、外部干扰以及模型不确定性时，仍能实现令人满意的系统性能。

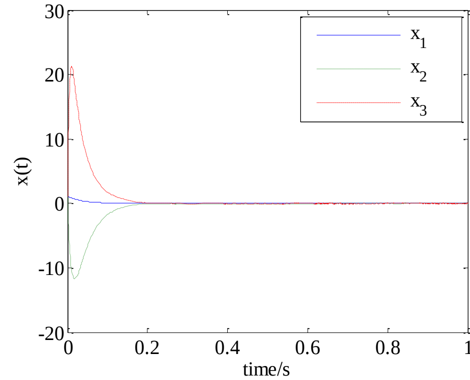


图 2　系统状态响应曲线图

Fig. 2　The response curves of system states

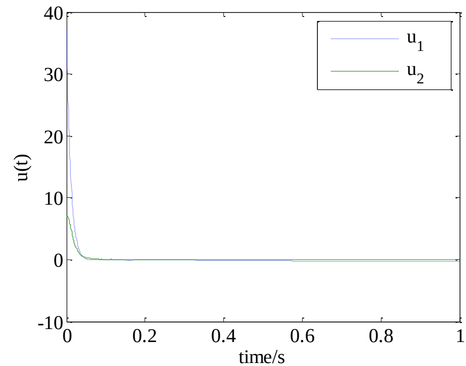


图 3　系统控制输入响应曲线图

Fig. 3　The response curves of control inputs

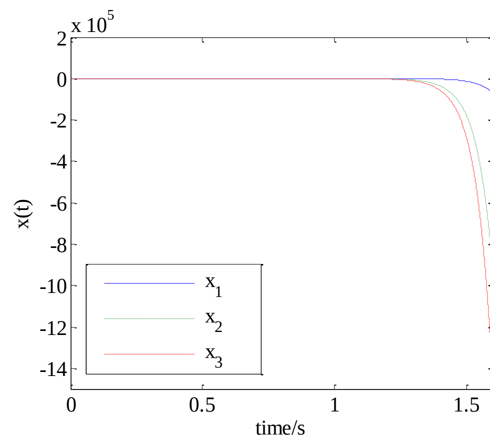


图 4　系统状态响应曲线图

Fig. 4　The response curves of system states

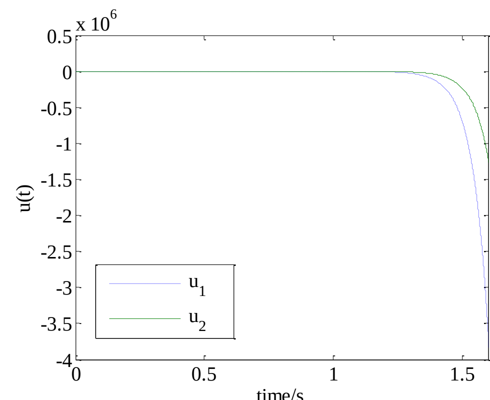


图 5　系统控制输入响应曲线图

Fig. 5　The response curves of control inputs

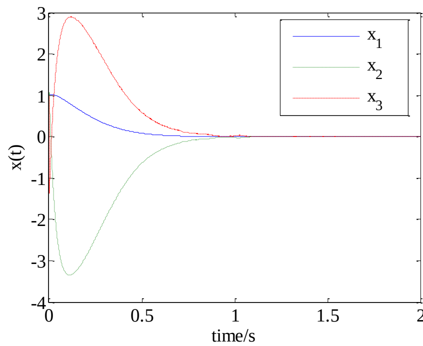


图 6　系统状态响应曲线图

Fig. 6　The response curves of system states

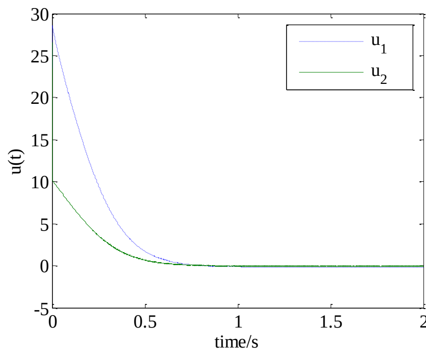


图 7　系统控制输入响应曲线图

Fig. 7　The response curves of control inputs

从上面三种情况的仿真效果对比表明，文献[12]设计的控制器能确保在发生情况 1 的信息物理系统，即量化匹配的信息物理系统，实现稳定，但当发生量化不匹配时，由仿真图 4 和 5 可以看出文献[12]的控制器已经无法确保信息物理系统的稳定，严重时甚至导致系统失稳。由情况②的仿真可以看出，本文设计的控制器能有效克服量化不匹配等的影响，确保信息物理系统的稳定，充分验证了本文控制算法的有效性和优越性。

4　结束语

本文研究了存在执行器攻击、外部干扰和量化不匹配的信息物理系统的安全控制问题。设计的控制器由线性和非线性两部分组成，其中，线性部分用于使模型不确定性系统实现 H_2 性能；其非线性部分用于消除外部干扰、量化误差以及抑制或抵消状态相关的执行器攻击对系统的影响，以确保闭环系统的一致最终有界性。仿真结果体现了文中算法的有效性与优越性。未来的研究工作中，将重点解决发生通信中断和时延等情形下的信息物理系统的安全可靠控制问题。

参考文献：

[1] 王中杰，谢璐璐. 信息物理融合系统研究综述 [J]. 自动化学报，2011，37(10):1157-1166. (Wang Zhongjie, Xie Lulu. Cyber-physical systems: A survey [J]. Acta Automatica Sinica, 2011, 37(10): 1157-1166.)

[2] Baheti R, Gill H. Cyber-physical systems [J]. The Impact of Control Technology, 2011, 12(1): 161-166.

[3] Burg A, Chattopadhyay A, Lam K Y. Wireless communication and security Issues for cyber–physical systems and the internet-of-things [J]. Proceedings of the IEEE, 2018, 106(1): 38-60.

[4] Chen Bo, Ho D W C, Hu Guoqiang, *et al.* Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks [J]. IEEE Trans on Cybernetics, 2018, 48(6): 1862-1876.

[5] Wolf M, Serpanos D. Safety and security in cyber-physical systems and internet-of-things systems [J]. Proceedings of the IEEE, 2018, 106(1): 9-20.

[6] 陈功谱，曹向辉，孙长银. 信息物理系统安全问题研究进展 [J]. 南京信息工程大学学报，2017，9(4)：372-380. (Chen Gongpu, Cao Xianghui, Sun Changyin. A survey on the security of cyber-physical systems [J]. Journal of Nanjing University of Information Science and Technology, 2017, 9(4): 372-380.)

[7] Giraldo J, Sarkar E, Cardenas A, *et al.* Security and privacy in cyber-physical systems: a survey of surveys [J]. IEEE Design & Test, 2017, 34(4): 7-17.

[8] Yucelen T, Haddad W M, Feron E M. Adaptive control architectures for mitigating sensor attacks in cyber-physical systems [J]. Cyber-Physical Systems, 2016, 2(1-4): 24-52.

[9] Xie Chunhua, Yang Guanghong. Secure estimation for cyber-physical systems under adversarial actuator attacks [J]. IET Control Theory & Applications, 2017, 11(17): 2939-2946.

[10] Jin Xu, Haddad W M, Yucelen T. An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems [J]. IEEE Trans on Automatic Control, 2017, 62(11): 6058-6064.

[11] 李炜，吴晰源，赵正天，等. 同时考虑量化误差的网络化控制系统鲁棒 H∞完整性设计 [J]. 计算机应用研究，2012, 29(6): 2120-2125. (Li Wei, Wu Xiyuan, Zhao Zhengtian, *et al.* Robust H∞ integrity design of networked control system with quantizing error [J]. Application Research of Computers, 2012, 29(6): 2120-2125.)

[12] Yun S W, Choi Y J, Park P G. H2 control of continuous-time uncertain linear systems with input quantization and matched disturbances [J]. Automatica, 2009, 45 (10): 2435-2439.

[13] Zheng Bochao, Yang Guanghong. H2 control of linear uncertain systems considering input quantization with encoder/decoder mismatch [J]. ISA Trans, 2013, 52(5): 577-582.

[14] 屈百达，胥吉林，徐保国. 不确定多时滞系统的鲁棒 H∞控制 [J]. 计算机应用研究，2012, 29(12): 4577-4579. (Qu Baida, Xu Jilin, Xu Baoguo. Robust H∞ control for uncertain systems with multiple time-delay [J]. Application Research of Computers, 2012, 29(12): 4577-4579.)

[15] Petersen I R. A stabilization algorithm for a class of uncertain linear systems [J]. Systems & Control Letters, 1987, 8(4): 351-357.